

The Plünnecke-Ruzsa Inequality

Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson

October 27, 2022

Abstract

We formalise Plünnecke's inequality and the Plünnecke-Ruzsa inequality, following the notes by Timothy Gowers: "Introduction to Additive Combinatorics" (2022) for the University of Cambridge. To this end, we first introduce basic definitions and prove elementary facts on sumsets and difference sets. Then, we show two versions of the Ruzsa triangle inequality. We follow with a proof due to Petridis [1].

Contents

1	The Plünnecke-Ruzsa Inequality	3
1.1	Key definitions (sumset, difference set) and basic lemmas . . .	3
1.1.1	Sumsets	3
1.1.2	Iterated sumsets	6
1.1.3	Difference sets	6
1.2	The Ruzsa triangle inequality	8
1.3	Petridis's proof of the Plünnecke-Ruzsa inequality	8
1.4	Supplementary material on sumsets for sets of integers: basic inequalities	10

Acknowledgements The authors were supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council.

1 The Plünnecke-Ruzsa Inequality

Authors: Angeliki Koutsoukou-Argraki and Lawrence C. Paulson, University of Cambridge.

We formalise Plünnecke's inequality and the Plünnecke-Ruzsa inequality, following the notes by Timothy Gowers: "Introduction to Additive Combinatorics" (2022) for the University of Cambridge. To this end, we first introduce basic definitions and prove elementary facts on sumsets and difference sets. Then, we show (two versions of) the Ruzsa triangle inequality. We follow with a proof due to Petridis.

```
theory Pluenecke-Ruzsa-Inequality
imports
  Jacobson-Basic-Algebra.Ring-Theory
  Complex-Main
```

```
begin
```

```
notation plus (infixl + 65)
notation minus (infixl - 65)
notation uminus (- - [81] 80)
```

1.1 Key definitions (sumset, difference set) and basic lemmas

Working in an arbitrary Abelian group, with additive syntax

```
locale additive-abelian-group = abelian-group  $G$  ( $\oplus$ )  $\mathbf{0}$ 
for  $G$  and addition (infixl  $\oplus$  65) and zero ( $\mathbf{0}$ )
```

```
begin
```

```
abbreviation G-minus:: 'a  $\Rightarrow$  'a  $\Rightarrow$  'a (infixl  $\ominus$  70)
where  $x \ominus y \equiv x \oplus \textit{inverse } y$ 
```

```
lemma inverse-closed:  $x \in G \implies \textit{inverse } x \in G$ 
  <proof>
```

1.1.1 Sumsets

```
inductive-set sumset :: 'a set  $\Rightarrow$  'a set  $\Rightarrow$  'a set for  $A B$ 
where
  sumsetI[intro]:  $\llbracket a \in A; a \in G; b \in B; b \in G \rrbracket \implies a \oplus b \in \textit{sumset } A B$ 
```

```
lemma sumset-eq:  $\textit{sumset } A B = \{c. \exists a \in A \cap G. \exists b \in B \cap G. c = a \oplus b\}$ 
  <proof>
```

```
lemma sumset:  $\textit{sumset } A B = (\bigcup a \in A \cap G. \bigcup b \in B \cap G. \{a \oplus b\})$ 
  <proof>
```

lemma *sumset-subset-carrier*: $\text{sumset } A \ B \subseteq G$

<proof>

lemma *sumset-Int-carrier [simp]*: $\text{sumset } A \ B \cap G = \text{sumset } A \ B$

<proof>

lemma *sumset-mono*: $[[A' \subseteq A; B' \subseteq B]] \implies \text{sumset } A' \ B' \subseteq \text{sumset } A \ B$

<proof>

lemma *sumset-insert1*: *NO-MATCH* $\{\} \ A \implies \text{sumset } (\text{insert } x \ A) \ B = \text{sumset } \{x\} \ B \cup \text{sumset } A \ B$

<proof>

lemma *sumset-insert2*: *NO-MATCH* $\{\} \ B \implies \text{sumset } A \ (\text{insert } x \ B) = \text{sumset } A \ \{x\} \cup \text{sumset } A \ B$

<proof>

lemma *sumset-subset-Un1*: $\text{sumset } (A \cup A') \ B = \text{sumset } A \ B \cup \text{sumset } A' \ B$

<proof>

lemma *sumset-subset-Un2*: $\text{sumset } A \ (B \cup B') = \text{sumset } A \ B \cup \text{sumset } A \ B'$

<proof>

lemma *sumset-subset-insert*: $\text{sumset } A \ B \subseteq \text{sumset } A \ (\text{insert } x \ B) \ \text{sumset } A \ B \subseteq \text{sumset } (\text{insert } x \ A) \ B$

<proof>

lemma *sumset-subset-Un*: $\text{sumset } A \ B \subseteq \text{sumset } A \ (B \cup C) \ \text{sumset } A \ B \subseteq \text{sumset } (A \cup C) \ B$

<proof>

lemma *sumset-empty [simp]*: $\text{sumset } A \ \{\} = \{\} \ \text{sumset } \{\} \ A = \{\}$

<proof>

lemma *sumset-empty'*:

assumes $A \cap G = \{\}$

shows $\text{sumset } B \ A = \{\} \ \text{sumset } A \ B = \{\}$

<proof>

lemma *sumset-is-empty-iff [simp]*: $\text{sumset } A \ B = \{\} \longleftrightarrow A \cap G = \{\} \vee B \cap G = \{\}$

<proof>

lemma *sumset-D [simp]*: $\text{sumset } A \ \{\mathbf{0}\} = A \cap G \ \text{sumset } \{\mathbf{0}\} \ A = A \cap G$

<proof>

lemma *sumset-Int-carrier-eq [simp]*: $\text{sumset } A \ (B \cap G) = \text{sumset } A \ B \ \text{sumset } (A \cap G) \ B = \text{sumset } A \ B$

<proof>

lemma *sumset-assoc:*

shows $\text{sumset } (\text{sumset } A B) C = \text{sumset } A (\text{sumset } B C)$

<proof>

lemma *sumset-commute:*

shows $\text{sumset } A B = \text{sumset } B A$

<proof>

lemma *finite-sumset:*

assumes *finite* A *finite* B **shows** *finite* $(\text{sumset } A B)$

<proof>

lemma *finite-sumset':*

assumes *finite* $(A \cap G)$ *finite* $(B \cap G)$

shows *finite* $(\text{sumset } A B)$

<proof>

lemma *sumsetdiff-sing:* $\text{sumset } (A - B) \{x\} = \text{sumset } A \{x\} - \text{sumset } B \{x\}$

<proof>

lemma *card-sumset-singleton-eq:*

assumes *finite* A **shows** $\text{card } (\text{sumset } A \{a\}) = (\text{if } a \in G \text{ then } \text{card } (A \cap G) \text{ else } 0)$

<proof>

lemma *card-sumset-le:*

assumes *finite* A **shows** $\text{card } (\text{sumset } A \{a\}) \leq \text{card } A$

<proof>

lemma *infinite-sumset-aux:*

assumes *infinite* $(A \cap G)$

shows $\text{infinite } (\text{sumset } A B) \longleftrightarrow B \cap G \neq \{\}$

<proof>

lemma *infinite-sumset-iff:*

shows $\text{infinite } (\text{sumset } A B) \longleftrightarrow \text{infinite } (A \cap G) \wedge B \cap G \neq \{\} \vee A \cap G \neq \{\} \wedge \text{infinite } (B \cap G)$

<proof>

lemma *card-le-sumset:*

assumes A : *finite* A $a \in A$ $a \in G$

and B : *finite* B $B \subseteq G$

shows $\text{card } B \leq \text{card } (\text{sumset } A B)$

<proof>

lemma *card-sumset-0-iff':* $\text{card } (\text{sumset } A B) = 0 \longleftrightarrow \text{card } (A \cap G) = 0 \vee \text{card } (B \cap G) = 0$

<proof>

lemma *card-sumset-0-iff*:

assumes $A \subseteq G \ B \subseteq G$

shows $\text{card} (\text{sumset } A \ B) = 0 \iff \text{card } A = 0 \vee \text{card } B = 0$

<proof>

lemma *card-sumset-leq*:

assumes $A \subseteq G$

shows $\text{card}(\text{sumset } A \ A) \leq \text{Suc}(\text{card } A)$ *choose 2*

<proof>

1.1.2 Iterated sumsets

definition *sumset-iterated* :: 'a set \Rightarrow nat \Rightarrow 'a set

where *sumset-iterated* $A \ r \equiv \text{Finite-Set.fold} (\text{sumset} \circ (\lambda-. A)) \ \{\mathbf{0}\} \ \{..<r\}$

lemma *sumset-iterated-0 [simp]*: *sumset-iterated* $A \ 0 = \{\mathbf{0}\}$

<proof>

lemma *sumset-iterated-Suc [simp]*: *sumset-iterated* $A \ (\text{Suc } k) = \text{sumset } A \ (\text{sumset-iterated } A \ k)$

(**is** ?lhs = ?rhs)

<proof>

lemma *sumset-iterated-2*:

shows *sumset-iterated* $A \ 2 = \text{sumset } A \ A$

<proof>

lemma *sumset-iterated-r*: $r > 0 \implies \text{sumset-iterated } A \ r = \text{sumset } A \ (\text{sumset-iterated } A \ (r-1))$

<proof>

lemma *sumset-iterated-subset-carrier*: *sumset-iterated* $A \ k \subseteq G$

<proof>

lemma *finite-sumset-iterated*: *finite* $A \implies \text{finite} (\text{sumset-iterated } A \ r)$

<proof>

lemma *sumset-iterated-empty*: $r > 0 \implies \text{sumset-iterated } \{\} \ r = \{\}$

<proof>

1.1.3 Difference sets

inductive-set *minusset* :: 'a set \Rightarrow 'a set **for** A

where

minussetI[intro]: $\llbracket a \in A; a \in G \rrbracket \implies \text{inverse } a \in \text{minusset } A$

lemma *minusset-eq*: *minusset* $A = \text{inverse} \ ` (A \cap G)$

<proof>

abbreviation *differenceset* $A B \equiv \text{sumset } A (\text{minusset } B)$

lemma *minusset-is-empty-iff* [simp]: $\text{minusset } A = \{\}$ $\longleftrightarrow A \cap G = \{\}$
<proof>

lemma *minusset-triv* [simp]: $\text{minusset } \{0\} = \{0\}$
<proof>

lemma *minusset-subset-carrier*: $\text{minusset } A \subseteq G$
<proof>

lemma *minus-minusset* [simp]: $\text{minusset } (\text{minusset } A) = A \cap G$
<proof>

lemma *card-minusset* [simp]: $\text{card } (\text{minusset } A) = \text{card } (A \cap G)$
<proof>

lemma *card-minusset'*: $A \subseteq G \implies \text{card } (\text{minusset } A) = \text{card } A$
<proof>

lemma *diff-minus-set*:
 $\text{differenceset } (\text{minusset } A) B = \text{minusset } (\text{sumset } A B)$ (is ?lhs = ?rhs)
<proof>

lemma *differenceset-commute* [simp]:
shows $\text{minusset } (\text{differenceset } B A) = \text{differenceset } A B$
<proof>

lemma *card-differenceset-commute*: $\text{card } (\text{differenceset } B A) = \text{card } (\text{differenceset } A B)$
<proof>

lemma *minusset-distrib-sum*:
shows $\text{minusset } (\text{sumset } A B) = \text{sumset } (\text{minusset } A) (\text{minusset } B)$
<proof>

lemma *minusset-iterated-minusset*: $\text{sumset-iterated } (\text{minusset } A) k = \text{minusset } (\text{sumset-iterated } A k)$
<proof>

lemma *card-sumset-iterated-minusset*:
 $\text{card } (\text{sumset-iterated } (\text{minusset } A) k) = \text{card } (\text{sumset-iterated } A k)$
<proof>

lemma *finite-minusset*: $\text{finite } A \implies \text{finite } (\text{minusset } A)$
<proof>

lemma *finite-differenceset*: $\text{finite } A \implies \text{finite } B \implies \text{finite } (\text{differenceset } A \ B)$
 ⟨proof⟩

1.2 The Ruzsa triangle inequality

lemma *Ruzsa-triangle-ineq1*:
assumes U : *finite* $U \subseteq G$
and V : *finite* $V \subseteq G$
and W : *finite* $W \subseteq G$
shows $(\text{card } U) * \text{card}(\text{differenceset } V \ W) \leq \text{card } (\text{differenceset } U \ V) * \text{card}(\text{differenceset } U \ W)$
 ⟨proof⟩

definition *Ruzsa-distance*:: 'a set \Rightarrow 'a set \Rightarrow real
where *Ruzsa-distance* $A \ B \equiv \text{card}(\text{differenceset } A \ B) / (\text{sqrt}(\text{card } A) * \text{sqrt}(\text{card } B))$

lemma *Ruzsa-triangle-ineq2*:
assumes U : *finite* $U \subseteq G \ U \neq \{\}$
and V : *finite* $V \subseteq G$
and W : *finite* $W \subseteq G$
shows *Ruzsa-distance* $V \ W \leq (\text{Ruzsa-distance } V \ U) * (\text{Ruzsa-distance } U \ W)$
 ⟨proof⟩

1.3 Petridis's proof of the Plünnecke-Ruzsa inequality

lemma *Plu-2-2*:
assumes $K0$: $\text{card } (\text{sumset } A \ 0 \ B) \leq K0 * \text{real } (\text{card } A0)$
and $A0$: *finite* $A0 \subseteq G \ A0 \neq \{\}$
and B : *finite* $B \subseteq G \ B \neq \{\}$
obtains $A \ K$
where $A \subseteq A0 \ A \neq \{\}$ $0 < K \ K \leq K0$
and $\bigwedge C. C \subseteq G \implies \text{finite } C \implies \text{card } (\text{sumset } A \ (\text{sumset } B \ C)) \leq K * \text{real}(\text{card}(\text{sumset } A \ C))$
 ⟨proof⟩

lemma *Cor-Plu-2-3*:
assumes K : $\text{card } (\text{sumset } A \ B) \leq K * \text{real } (\text{card } A)$
and A : *finite* $A \subseteq G \ A \neq \{\}$
and B : *finite* $B \subseteq G$
obtains A' **where** $A' \subseteq A \ A' \neq \{\}$
 $\bigwedge r. \text{card } (\text{sumset } A' \ (\text{sumset-iterated } B \ r)) \leq K \hat{\ } r * \text{real } (\text{card } A')$
 ⟨proof⟩

The following Corollary of the above is an important special case, also referred to as the original version of Plünnecke's inequality first shown by Plünnecke.

lemma *Cor-Plu-2-3-Pluenecke-ineq*:

assumes $K: \text{card}(\text{sumset } A B) \leq K * \text{real}(\text{card } A)$
and $A: \text{finite } A \ A \subseteq G \ A \neq \{\}$
and $B: \text{finite } B \ B \subseteq G$
shows $\text{real}(\text{card}(\text{sumset-iterated } B r)) \leq K \wedge r * \text{real}(\text{card } A)$
 <proof>

Special case where $B = A$

lemma *Cor-Plu-2-3-1*:
assumes $K: \text{card}(\text{sumset } A A) \leq K * \text{real}(\text{card } A)$
and $A: \text{finite } A \ A \subseteq G \ A \neq \{\}$
shows $\text{card}(\text{sumset-iterated } A r) \leq K \wedge r * \text{real}(\text{card } A)$
 <proof>

Special case where $B = - A$

lemma *Cor-Plu-2-3-2*:
assumes $K: \text{card}(\text{differenceset } A A) \leq K * \text{real}(\text{card } A)$
and $A: \text{finite } A \ A \subseteq G \ A \neq \{\}$
shows $\text{card}(\text{sumset-iterated } A r) \leq K \wedge r * \text{real}(\text{card } A)$
 <proof>

The following result is known as the Plünnecke-Ruzsa inequality (Theorem 2.5 in Gowers's notes). The proof will make use of the Ruzsa triangle inequality.

theorem *Pluenncke-Ruzsa-ineq*:
assumes $K: \text{card}(\text{sumset } A B) \leq K * \text{real}(\text{card } A)$
and $A: \text{finite } A \ A \subseteq G \ A \neq \{\}$
and $B: \text{finite } B \ B \subseteq G$
and $0 < r \ 0 < s$
shows $\text{card}(\text{differenceset}(\text{sumset-iterated } B r) (\text{sumset-iterated } B s)) \leq K \wedge (r+s) * \text{real}(\text{card } A)$
 <proof>

The following is an alternative version of the Plünnecke-Ruzsa inequality (Theorem 2.1 in Gowers's notes).

theorem *Pluenncke-Ruzsa-ineq-alt*:
assumes $\text{finite } A \ A \subseteq G$
and $\text{card}(\text{sumset } A A) \leq K * \text{real}(\text{card } A) \ r > 0 \ s > 0$
shows $\text{card}(\text{differenceset}(\text{sumset-iterated } A r) (\text{sumset-iterated } A s)) \leq K \wedge (r+s) * \text{real}(\text{card } A)$
 <proof>

theorem *Pluenncke-Ruzsa-ineq-alt-2*:
assumes $\text{finite } A \ A \subseteq G$
and $\text{card}(\text{differenceset } A A) \leq K * \text{real}(\text{card } A) \ r > 0 \ s > 0$
shows $\text{card}(\text{differenceset}(\text{sumset-iterated } A r) (\text{sumset-iterated } A s)) \leq K \wedge (r+s) * \text{real}(\text{card } A)$
 <proof>

end

1.4 Supplementary material on sumsets for sets of integers: basic inequalities

lemma *moninv-int: monoid.invertible UNIV (+) 0 u for u::int*
<proof>

interpretation *int: additive-abelian-group UNIV (+) 0::int*
<proof>

lemma *card-sumset-geq1:*
assumes *A: A ≠ {} finite A and B: B ≠ {} finite B*
shows *card(int.sumset A B) ≥ (card A) + (card B) - 1*
<proof>

lemma *card-sumset-geq2:*
shows *card(int.sumset A A) ≥ 2 * (card A) - 1*
<proof>

end

References

- [1] G. Petridis. The Plünnecke–Ruzsa inequality: An overview. In M. B. Nathanson, editor, *Combinatorial and Additive Number Theory*, pages 229–241. Springer, 2014.